INTRODUCTION: GIAC ENTERPRISES

• World’s largest supplier of fortune-cookie sayings
• E-commerce site for fortune orders
• Cookie sayings submission via mobile app; stored in MySQL Database that is highest value asset
• Log volume is too high for manual analysis, need low-cost SIEM solution
GIAC ARCHITECTURE

- Two datacenters, each with:
  - Apache web servers
  - MySQL database backend
  - HAProxy
  - Web Application Firewall
  - Cisco Firewall and Switches/Routers
  - Mobile Device Management for employee/contractor BYOD
  - Active Directory Infrastructure
- Employee/contractors:
  - Primarily Windows desktops
  - Contractor-owned systems for fortune submission
IMPORTANT FEATURES

• Windows and Linux log support
• Active open source community
• Log correlation
• Threat Feeds
• Role-based Access Control
• Long-term log storage
POC ARCHITECTURE

NAT Gateway
MySQL DB
Apache Webservers
Active Directory
Infrastructure Servers
OSSIM Control Node

192.168.0.0/24
192.168.2.0/24
INSTALLATION & CONFIGURATION

• Installs from ISO image
• Conversion process for use in AWS
• Setup configures interfaces and initial accounts
• Wizard for easy configuration
• Initial asset & network discovery
DATA SOURCES

- Windows Event Logs
- OSSEC Rootkit Detection & File Change Monitoring
- Linux Syslog
- Apache Logs
- Database Logs
- Vulnerability Scans
- Open Threat Exchange
- NMAP
LOGGING CONFIGURATION

• Log data parsed & normalized via plugins
• Most can be configured via wizard or web interface
• Some require console “Jailbreak” to enable
  • Rsyslog
  • Database plugins
VULNERABILITY SCANS

• Can be run ad-hoc or scheduled
• Configured to run against specific asset group
• Credentialed & Unauthenticated
• Built-in default scans or full customization of checks
OPEN THREAT EXCHANGE

• OTX “Pulses” contain community-updated source of current threat data
• Can subscribe to single Pulse or user feed
• Pulses Contain Indicators of Compromise
  • IP addresses, URLs, domain data
  • File hashes
  • Geographical data
• Tagged by OS, software
TICKET SYSTEM

• Opened automatically for vulnerabilities or alarms above a configured severity threshold
• Can be updated, re-assigned, and have status or priority changed
• Ability to close as false positives
STRENGTHS AND WEAKNESSES

• Supports many of GIAC’s data sources out of the box
• Highly configurable; allows customized plugins, rules, severities
• Good documentation and online support resources
• Vulnerability scanning with update
• HIDS capabilities

• Resource-intensive; requires lots of memory and CPU to support
• Open Threat Exchange potentially powerful capability, but not easy to use well
• Limited reporting capabilities
NEXT STEPS

• Configure TLS for log sources
• Add ELK stack for long-term log storage
• Tune logs and alerting:
  • to reduce false positives
  • improve performance
• Create plugins for unsupported sources
• Investigate active-response capabilities
CONCLUSION

• Successful Proof of Concept, should move forward with full deployment
  • Supports major GIAC use cases out of the box
  • Potential solution for long-term log storage
  • Highly flexible system
  • Enterprise solution available if support needed
### Upcoming SANS Training

<table>
<thead>
<tr>
<th>Course</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virgin Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>New Orleans, LAUS</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>